Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Symbolic Computation 39 (2005) 617–630
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Factoring polynomials over global fields I

Michael E. Pohst*

Technische Universität Berlin, Institut für Mathematik-MA 8-1, Straße des 17. Juni 136, 10623 Berlin, Germany

Received 17 November 1998; accepted 20 September 2004
Available online 10 December 2004

Abstract

In this paper we present a generic algorithm for factoring polynomials over global fields F. As efficient implementations of that algorithm for number fields and function fields differ substantially, these cases will be treated separately. Complexity issues and implementations will be discussed in part II which also contains illustrative examples.

Keywords: Polynomial factorization; Global fields

1. A generic algorithm

It seems to be common knowledge that algorithms for factoring polynomials over algebraic number fields K are comparatively slow. Practically all methods in use (i.e., which are implemented in a computer algebra system) have the – at least – theoretical disadvantage that they try to avoid arithmetic in K. They either transform the task into a polynomial factorization over $\mathbb{Q}$ of a polynomial of much higher degree or they imitate residue class arithmetic for ideals by residue class arithmetic of polynomials. With powerful algebraic number field packages at hand, this approach no longer seems to be adequate.

* Tel.: +49 30 314 25772; fax: +49 30 314 21604.
E-mail address: pohst@math.tu-berlin.de.

0747-7171/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2004.09.006

Apart from the first paper on this subject by Weinberger and Rothschild (1976), nowadays two methods prevail. The first one goes back to Trager (1976) and was recently improved by Encarnación (1997). It is based on factoring the norm of the given polynomial over $\mathbb{Q}$, i.e., the underlying number field is eliminated at the cost of a large increase in the degree of the polynomial. The second method is due to Lenstra (1982). He also eliminates the number field and performs arithmetic in residue class rings modulo suitable polynomials. The transition of a factorization in a residue class ring to the original ring is then via lattice basis reduction. In Lenstra's paper only the basic ideas are sketched.

In principle, we follow his ideas inasmuch as they provide a canonical generalization of the standard factorization method over $\mathbb{Q}$ to all global fields K. This becomes clear when one replaces his residue class rings by residue class rings modulo a power of a maximal ideal of the ring of integers in K. If that ideal is chosen appropriately, the arithmetic in the corresponding residue class rings becomes quite simple and the whole method therefore efficient. We emphasize that for number fields our interpretation of the generic algorithm already differs a lot from Lenstra's algorithm (see also below). For function fields in one variable over a finite field the entire algorithm is new. It became possible to develop it only after the necessary tools from the geometry of numbers for function fields became available (Schörnig, 1996).

Let K be an arbitrary field and $g(t) = \sum_{i=0}^{m} g_i t^i \in K[t]$ a univariate polynomial of degree $m = \deg(g) > 1$. One of the basic tasks of computational algebra is to develop methods for factoring $g(t)$ into a product of irreducible polynomials. Obviously, if $g(t)$ is reducible this task can be reduced to the problem of determining a factorization $g(t) = h(t)k(t)$ with polynomials $h(t), k(t) \in K[t]$ and $0 < \deg(h), \deg(k) < \deg(g)$. Our goal is to develop an algorithm for the latter problem. Over arbitrary fields K we can obtain a factorization of $g(t)$ into a product of square-free polynomials with the following ideas. If $h(t)^2$ divides $g(t)$, then $h(t)$ divides the derivative $g'(t)$ of $g(t)$ in $K[t]$. In the case where $g'(t)$ is not zero the Euclidean algorithm applied to $g(t)$ and $g'(t)$ yields a proper factor of $g(t)$. If $g'(t)$ is zero, however, K is necessarily of finite characteristic, say p, and in $g(t)$ every power of t with a non-zero coefficient is a p-th power. This again leads to a simplification of the task. In the following we therefore make the assumption that

(A1) $g(t)$ is square-free.

Since there is no algorithm known with which $g(t)$ can be factored over arbitrary fields we need to add conditions on K. Guided by ideas from the factorization of polynomials over the rational numbers we assume that

(A2) K is the quotient field of a suitable integral domain R.

We note that K should therefore not be finite. Then there is the following generic algorithm.

Generic Factorization Algorithm.
Input An integral domain R with quotient field K and a square-free polynomial $g(t) \in K[t]$ of degree greater than one.

Output A factorization of $g(t)$ in $K[t]$.

Step 1. Choose an appropriate maximal ideal $\mathfrak{m}$ of R.

Step 2. Factor $g(t)$ in $R/\mathfrak{m}[t]$.

Step 3. Lift the factorization of Step 2 to a factorization in $R/\mathfrak{m}^k\,[t]$ for a sufficiently large exponent k.

Step 4. Recover a factorization in $K[t]$ from the factorization of Step 3.

Remark. If F is an algebraic number field this algorithm essentially coincides with that in Lenstra (1982), though ideals are never mentioned in his paper. Our use of ideal arithmetic (for ideals of degree one) rather than polynomial arithmetic yields a much faster implementation. It also helps to view this algorithm as a generalization of the factorization algorithm for $\mathbb{Q}$. The two subsequent sections on the algorithm for number fields can therefore be considered as new ideas for an improvement and a more efficient implementation of the basic idea of Lenstra's algorithm. We point out that our methods used for Steps 1–4 have no analogy in Lenstra's paper. We not only exchange polynomial arithmetic and ideal arithmetic, we also use a completely different size function for Step 4.

Before we discuss the four steps of our algorithm in some detail, we note that the problem of factoring $g(t)$ over the field K is transferred to the problem of factoring $g(t)$ over the field $R/\mathfrak{m}$. We only get an advantage if the latter task is easier than the previous one. This will usually be the case if $R/\mathfrak{m}$ is a finite field. Therefore we only consider global fields in this paper.

In Step 1 the choice of the maximal ideal $\mathfrak{m}$ is subject to several side conditions. Clearly, the denominators of all coefficients of $g(t)$ must not lie in $\mathfrak{m}$ in order that the image of $g(t)$ in $R/\mathfrak{m}\,[t]$ is well defined. Since the degree of that image should equal the degree of $g(t)$, the numerator of the leading coefficient of $g(t)$ must also not be in $\mathfrak{m}$. Eventually, the factorization of $g(t)$ in $R/\mathfrak{m}\,[t]$ must not contain multiple factors (see the remarks concerning Step 3). This will be satisfied if the discriminant of $g(t)$ is not contained in $\mathfrak{m}$. Besides these theoretical aspects, the map from R onto $R/\mathfrak{m}$ and the arithmetic in $R/\mathfrak{m}$ should be easy from a computational point of view. Hence, we suggest choosing maximal ideals of degree one (see Section 3).

As regards Step 2, we already mentioned that factoring the image of $g(t)$ in $R/\mathfrak{m}\,[t]$ should be much simpler than factoring $g(t)$ in $K[t]$. Polynomial factorization over small finite fields is known to be relatively fast. Therefore we would like $R/\mathfrak{m}$ to be a small finite field. Then we can apply the usual factorization methods based on ideas of Berlekamp or Cantor–Zassenhaus (see Bach and Shallit (1996), for example).

The lifting procedure of Step 3 is well known as Hensel Lifting. It can be carried out over arbitrary commutative unital rings R provided that the factors of $g(t)$ obtained in Step 2 are coprime. A detailed discussion of that method can be found in Pohst and Zassenhaus (1989).

Finally, Step 4 is the crucial part of the algorithm. We recall a few facts from polynomial factorization over the rational integers. From the coefficients of a polynomial $g(t) \in \mathbb{Z}[t]$, bounds for the (complex) zeros of $g(t)$ are obtained. These then yield an upper bound B for the absolute value of any coefficient of a potential factor of $g(t)$ in $\mathbb{Z}[t]$. In this case the maximal ideal $\mathfrak{m}$ is of the form $p\mathbb{Z}$ with a prime number p. Without loss of generality we assume that p is odd. Let $h_1(t) \bmod p, \ldots, h_r(t) \bmod p$ be the coprime factors of $g(t)$ obtained in Step 2 and $h_{1k}(t) \bmod p^k, \ldots, h_{rk}(t) \bmod p^k$ the corresponding lifted

factors of Step 3, all having integer coefficients in the interval $]-p^k/2,\ p^k/2[$. If $p^k/2$ is larger than B, any factor of $g(t)$ in $\mathbb{Z}[t]$ is then a product mod p^k of 1 up to r factors $h_{ik}(t)$. Hence, a factorization of $g(t)$ in $\mathbb{Z}[t]$ can be recovered from one modulo p^k.

In the general situation of the generic algorithm we therefore need an appropriate size function that will replace the absolute value, i.e., for which a factor obtained in Step 3 corresponds to at most one actual factor of $g(t)$ and in which case the latter can indeed be calculated.

There is one additional difficulty. A factorization over the rational integers and a factorization over $\mathbb{Q}$ are equivalent according to Gauss's lemma since $\mathbb{Z}$ is a unique factorization domain. For the rings R that we consider this is not true in general. Factorizations of $g(t)$ over R and over K can differ substantially. For global fields the concept of algebraic integers can be used to solve this problem. A more general concept would work over valuation rings.

Remark. It is well known that the number of potential factors to be tested in Step 4 can grow exponentially with the degree of $g(t)$. In practice, this barely happens and can usually be avoided by making a suitable choice of $\mathfrak{m}$. In Lenstra et al. (1982) the authors show how lattice basis reduction methods can be used to get a factorization method over $\mathbb{Q}$ in polynomial time. These ideas can be transferred to global fields, too, but this will not be discussed in this paper.

To make the presentation easier, we shall impose two further assumptions on the polynomial to be factorized.

(A3) $g(t) \in R[t]$.

If this is not the case, we simply multiply $g(t)$ by the least common multiple (or simply the product) of the denominators of all non-zero coefficients.

(A4) $g(t)$ is monic.

Also, with the assumptions (A3) and (A4) the following discussions become much easier, especially for global fields. Any zero of $g(t)$ is then an algebraic integer, and therefore also the potential factors $h(t), k(t)$ will be monic and will have integer coefficients. For non-maximal orders R of K the investigation of potential denominators can be quite cumbersome.

Although the factoring algorithm that we develop in this paper works in algebraic number fields and in function fields of one variable over finite fields, the implementations in the two cases differ substantially. Hence, in the first part of this paper we present the underlying ideas in the number field case. In Section 3 we discuss the use of maximal ideals of degree one for number and function fields. In Section 4 we adapt the generic algorithm to global function fields. The efficiency of the actual implementations in the software system KANT/KASH will be discussed in a forthcoming paper by J. Mendez and the author.

2. The algorithm for number fields

Throughout this section and the subsequent one, F denotes an algebraic number field of degree n over the rational numbers $\mathbb{Q}$. We assume that it is generated by a root ρ of a

monic irreducible polynomial

$$f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbb{Z}[t].$$

Over the complex numbers $\mathbb{C}$ the polynomial $f(t)$ splits into a product of linear factors:

$$f(t) = \prod_{j=1}^{n} (t - \rho^{(j)}),$$

where the conjugates $\rho = \rho^{(1)}, \ldots, \rho^{(n)}$ are ordered as usual, i.e., $\rho^{(1)}, \ldots, \rho^{(r_1)} \in \mathbb{R}$ and $\rho^{(r_1+1)}, \ldots, \rho^{(n)} \in \mathbb{C} \setminus \mathbb{R}$ subject to $\rho^{(r_1+j)} = \overline{\rho^{(r_1+r_2+j)}}$ $(1 \le j \le r_2)$. ($\overline{\rho}$ denotes the complex conjugate of ρ.) In particular, we have

$$n = r_1 + 2r_2.$$

Any element α of F can be represented as a linear combination of $1, \rho, \ldots, \rho^{n-1}$ with rational coefficients. Substituting $\rho^{(j)}$ for ρ in that representation, we obtain the j-th conjugate $\alpha^{(j)}$ of α $(1 \le j \le n)$. Arithmetical problems usually require computations with algebraic integers contained in F, i.e., those elements of F whose minimal polynomials have coefficients in $\mathbb{Z}$. They form a ring o_F with a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ (the integral basis of F), the so-called maximal order of F. We can always take $\omega_1 = 1$ and $\omega_2 = \rho$, the latter by means of an appropriate choice of the generating element ρ. In the following we fix an integral basis of F with this property. Any element β of F is then representable by a vector of n rational numbers via

$$\beta = \sum_{i=1}^{n} b_i \omega_i \quad (b_i \in \mathbb{Q}).$$

We note that β is in o_F precisely if all b_i are rational integers.

In order to apply methods from the geometry of numbers, we equip F with a scalar product in the usual way:

$$< , >: F \times F \to \mathbb{R} \ : \ (\alpha, \beta) \ \mapsto \ \sum_{j=1}^{n} \alpha^{(j)} \overline{\beta^{(j)}}.$$

Representing α, β in the basis $\omega_1, \ldots, \omega_n$ of o_F, $< , >$ becomes a non-degenerate symmetric bilinear form with coefficient matrix (Gram matrix)

$$A = (< \omega_i, \ \omega_j >)_{1 \le i, j \le n}.$$

Clearly, the pair (o_F, A) is an n-dimensional lattice. For brevity, we set

$$T_2 \ : \ F \to \mathbb{R}^{\ge 0} \ : \ \alpha \ \mapsto < \alpha, \alpha >.$$

To discuss the problem of factoring a polynomial $g(t) \in F[t]$ of degree $m > 1$ in an arithmetic context, we assume without loss of generality (see Section 1) that $g(t)$ is monic and has coefficients in o_F. As we already pointed out in Section 1, for any factorization $g(t) = h(t)k(t)$ in $F[t]$ the factors $h(t), k(t)$ are in $o_F[t]$. Such a factorization is also

preserved under conjugation: $g^{(j)}(t) = h^{(j)}(t)k^{(j)}(t)$ in $F^{(j)}[t]$. From the coefficients of $g(t)$ we obtain bounds for the absolute values of the zeros of $g(t)$ and thus for the absolute values of the coefficients of a factor $h(t)$ in the usual way (Mignotte, 1974).

Lemma 2.1. *Let $g(t) = \sum_{i=0}^{m} g_i t^i \in o_F[t]$ be monic. If $h(t) = \sum_{i=0}^{r} h_i t^i \in o_F[t]$ is monic and divides $g(t)$, then its coefficients are bounded by*

$$| h_i | \leq \binom{r-1}{i} \left(\sum_{i=0}^{m} | g_i |^2 \right)^{1/2} + \binom{r-1}{i-1}.$$

Remark. Better bounds are known (see Beauzamy (1992), for example). They are not as easy to state, and in general the improvements have little impact on the running time of the algorithm. There is, however, one exception. If we are looking for factors of degree one or two only, then well-known numerical estimates for the roots of a polynomial are definitely superior. The following bounds for any root ξ of a non-constant polynomial $\sum_{i=0}^{r} h_i t^i \in \mathbb{C}[t]$ are usually the best ones (see (5.5.8) in Stoer and Bulirsch (1993)):

$$| \xi | \leq 2 \max \left\{ \sqrt[i]{\left| \frac{h_{r-i}}{h_r} \right|} \;\middle|\; 1 \leq i \leq r \right\}. \tag{1}$$

This observation is very important for tests of isomorphy between two number fields, where it must be decided whether a generating polynomial for the second field has a zero in the first one.

In any case we obtain upper bounds for the coefficients of each of the conjugate factors $h^{(j)}(t)$ and consequently an upper bound B for the T_2-values of the coefficients of a potential factor $h(t)$ of $g(t)$ in $o_F[t]$. That bound B can depend on the degree of $h(t)$ and consequently lead to early abort strategies if we are only interested in factors of small degree.

For our factoring algorithm we choose an appropriate prime ideal $\mathfrak{q}$ of degree 1 of o_F. As we already noted in Section 1, the discriminant $d(g)$ of $g(t)$ must not be contained in $\mathfrak{q}$, and we also require $2 \notin \mathfrak{q}$. Then $o_F/\mathfrak{q}$ is a finite field of $q = N(\mathfrak{q})$ elements and ρ is congruent to an element of $0, 1, \ldots, q-1$ modulo $\mathfrak{q}$. The transition matrix for sending the fixed integral basis $\omega_1, \ldots, \omega_n$ to a suitable $\mathbb{Z}$-basis of $\mathfrak{q}$ can be chosen as a matrix with diagonal elements $q, 1, \ldots, 1$, all elements off the diagonal in rows 2 to n being zero and the entries off the diagonal in row 1 lying in the interval $]-q/2, q/2[$. In the next section we will show that the computations required by the generic factorization algorithm are quite simple for prime ideals of degree one.

In the remainder of this section we consider the recovering procedure of Step 4 for number fields.

Lemma 2.2. *Let B be a constant greater than 1. For $k \geq n \log(4B/n)/(2\log(q))$ every residue class of $o_F/\mathfrak{q}^k$ contains at most one element α with $T_2(\alpha) < B$.*

Proof. Let $\alpha, \beta \in o_F$ satisfy $\alpha + \mathfrak{q}^k = \beta + \mathfrak{q}^k$, $\alpha \neq \beta$, $T_2(\alpha) \leq T_2(\beta)$. Clearly, $\alpha - \beta$ is in $\mathfrak{q}^k$ and therefore its absolute norm is at least q^k. By the inequality between arithmetic

and geometric means we obtain

$$q^k \leq |N(\alpha-\beta)| \leq \left(\frac{T_2(\alpha-\beta)}{n}\right)^{n/2}$$

and therefore

$$nq^{2k/n} \leq T_2(\alpha-\beta) \leq 4T_2(\beta). \quad \square$$

Elements of small T_2-value in residue classes of $o_F/\mathfrak{q}^k$ can be computed with the methods described in Pohst (1993).

Remarks. (i) Roblot developed a similar strategy in his thesis (Roblot, 1997). Following Lenstra's ideas, he shows that the first element of a LLL-reduced basis of an – in general larger – power of the ideal $\mathfrak{q}$ yields an element of minimal T_2-norm. In practice, it turned out that the biggest part of the computation time is consumed by the calculation of a LLL-reduced basis of $\mathfrak{q}^k$, whereas the calculation of an element of small T_2-norm in a residue class is negligible afterwards. Hence, we prefer to use a smaller power of the ideal.

(ii) In the case where F is not totally real, the Gram matrix A of the lattice considered has entries that are algebraic integers but not necessarily rational integers. Numerical experience indicates that it is likely that existing real implementations of the LLL algorithm encounter precision problems and a – sometimes superfluous – increase of the numerical precision is costly. Also the scalar products of the basis vectors of $\mathfrak{q}^k$ are essentially determined by their constant terms for increasing k. This inspired Fieker and Friedrichs (2000) to consider a different size function with values in the non-negative rational integers. They consider the maximal order o_F as a $\mathbb{Z}$-module and make use of the $\mathbb{Z}$-module isomorphism

$$\varphi : o_F \to \mathbb{Z}^n : x = \sum_{i=1}^{n} \xi_i \omega_i \mapsto (\xi_1, \ldots, \xi_n)^{tr},$$

where $\omega_1, \ldots, \omega_n$ is the fixed basis of o_F which was introduced above. Hence, we obtain another norm on o_F:

$$\|x\| = \left\| \sum_{i=1}^{n} \xi_i \omega_i \right\| = \left(\sum_{i=1}^{n} \xi_i^2 \right)^{1/2}.$$

In the vector space $\mathbb{R}^n$ all norms are equivalent. Hence, if $x \in o_F$ has a small T_2-value, it will have a comparatively small value $\|x\|$ and vice versa. These estimates can easily be made quantitative via $(x^{(1)}, \ldots, x^{(n)}) = (\xi_1, \ldots, \xi_n)\tilde{A}$, where the regular matrix $\tilde{A} = (\tilde{a}_{ij}) \in \mathbb{C}^{n\times n}$ has entries $\tilde{a}_{ij} = \omega_i^{(j)}$. We note that $\overline{\tilde{A}}\tilde{A}^{tr} = A$ is the Gram matrix of o_F. These ideas are carried through in detail in Fieker and Friedrichs (2000). Their application led to a considerable speed-up for non-totally real fields F.

Factorization Algorithm for Number Fields.
Input An algebraic number field F and a monic square-free polynomial $g(t) \in o_F[t]$ of degree $m > 1$.

Output A proper factor $h(t) \in o_F[t]$ of $g(t)$, or the message "$g(t)$ is irreducible".

Step 1. Choose a suitable prime ideal $\mathfrak{q}$ of degree 1 in o_F. Compute an upper bound B for the T_2-values of the coefficients of a potential factor $h(t)$ of $g(t)$ in $o_F[t]$. Calculate k according to the preceding lemma.

Step 2. Factor $g(t)$ modulo $\mathfrak{q}[t]$. If $g(t)$ remains irreducible modulo $\mathfrak{q}$, print "$g(t)$ is irreducible" and terminate. Otherwise Steps 3 and 4 need to be carried out for each proper factor of $g(t)$ modulo $\mathfrak{q}[t]$.

Step 3. Lift the factorization $g(t) \equiv h(t)k(t) \bmod \mathfrak{q}[t]$ of Step 2 to a congruence factorization modulo $\mathfrak{q}^k$. The polynomials obtained are again denoted by $h(t), k(t)$.

Step 4. For each coefficient ν of $h(t)$ calculate an element $\mu \in \nu + \mathfrak{q}^k$ of T_2-value bounded by B, if it exists. If there is no such element, we discard the polynomial $h(t)$. Otherwise we obtain a polynomial $\tilde{h}(t)$ that is congruent to $h(t)$ modulo $\mathfrak{q}^k$ and whose coefficients have "small" T_2-values. In that case we test whether $\tilde{h}(t)$ divides $g(t)$ in $o_F[t]$. In this way we either obtain a proper factor of $g(t)$, or, after an unsuccessful test of all $h(t)$ found in Step 2, we have proven that $g(t)$ is irreducible.

Remarks. (i) Of course, the prime ideal $\mathfrak{q}$ is to be chosen such that there exist few factors of $g(t)$ modulo $\mathfrak{q}$ (if possible). We suggest factoring the polynomial under consideration for up to five prime ideals of degree 1.

(ii) To find appropriate prime ideals, we recommend factoring the generating polynomial $f(t)$ modulo a few prime numbers q which have the size of half a word of the computer being used. In this way, residue class arithmetic is still as fast as possible and prime ideals of degree 1 are easier to find than starting with prime numbers right from the beginning.

(iii) During the lifting procedure, coefficients (of potential factors $h(t)$) with small T_2-values can be detected at an earlier stage (and superfluous candidates can be removed).

3. First-degree prime ideals

The lifting procedure of Step 3 of the algorithm requires arithmetic with prime ideals of degree 1 and with powers of them. The special degree property helps to speed up all computations considerably. This will be outlined in this section. The material presented has led to a considerable speed-up of calculations with first-degree prime ideals in KANT (Daberkow et al., 1997). We use the notation introduced for number fields and discuss the necessary changes for global function fields at the end of this section.

Let $\mathfrak{q}$ be a prime ideal of degree 1 in o_F, as in the previous section; i.e., $\mathfrak{q}$ contains neither 2 nor d_F and the norm q of $\mathfrak{q}$ is a prime number. Hence, there exist rational integers t_k that are uniquely determined modulo q^k such that $\rho + t_k \in \mathfrak{q}^k$ for all positive exponents k. Furthermore, $\mathfrak{q}^k$ has a $\mathbb{Z}$-basis

$$\tau_1^{(k)} = q^k,\ \tau_2^{(k)} = \rho + t_k,\ \tau_{i+1}^{(k)} = \rho\,\tau_i^{(k)}\quad (2 \le i \le n-1).$$

We note that an alternative basis is

$$\tilde{\tau}_i^{(k)} = \omega_i + t_i^{(k)} \quad (2 \le i \le n) \text{ and } \tilde{\tau}_1^{(k)} = q^k.$$

The rational integers $t_i^{(k)}$ $(2 \le i \le n)$ are again uniquely determined modulo q^k. Also we have $t_2^{(k)} = t_k$. In the following we therefore choose $t_i^{(k)}$ subject to

$$-q^k/2 \ < \ t_i^{(k)} \ < \ q^k/2 \ \ (2 \le i \le n, \ k \in \mathbb{N}). \tag{2}$$

This choice has the following consequences.

Lemma 3.1. *$j < k$ implies $t_i^{(k)} \equiv t_i^{(j)}$ modulo q^j.*

Proof. Clearly, the differences $t_i^{(k)} - t_i^{(j)} = \tilde{\tau}_i^{(k)} - \tilde{\tau}_i^{(j)}$ are in $\mathfrak{q}^j \cap \mathbb{Z} = q^j\mathbb{Z}$. □

Lemma 3.2. *For $j, \nu \in \mathbb{N}$ the quotients $\psi_i := (t_i^{(j+\nu)} - t_i^{(j)})/q^j$ $(2 \le i \le n)$ are in the interval $]-q^\nu/2, \ q^\nu/2[$.*

Proof. (i) The bounds (2) for $t_i^{(j+\nu)}$ yield the inequalities

$$-q^{j+\nu}/2 \ < \ t_i^{(j)} + q^j\psi_i \ < \ q^{j+\nu}/2,$$

and therefore

$$-(q^\nu+1)/2 < -q^\nu/2 - t_i^{(j)}/q^j < \psi < q^\nu/2 - t_i^{(j)} + q^j < (q^\nu+1)/2,$$

so ψ_i must lie in the interval stated in the lemma.

(ii) On the other hand, if we choose ψ_i within the given bounds, then we obtain for $t_i^{(j+\nu)}$

$$\begin{aligned} t_i^{(j+\nu)} \ &\le \ \lfloor q^j/2 \rfloor + q^j \lfloor q^\nu/2 \rfloor = (q^j-1)/2 + q^j(q^\nu-1)/2 \\ &= (q^{j+\nu}-1)/2 \ < \ q^{j+\nu}/2, \end{aligned}$$

and similarly

$$t_i^{(j+\nu)} \ > \ -q^{j+\nu}/2,$$

and hence the bounds of (2). □

Corollary 3.1. *There is a unique element $t_i^{(j,\nu)} \in \ ]-q^\nu/2, \ q^\nu/2[$ such that $\tau_i^{(j+\nu)} = \tau_i^{(j)} + q^j t_i^{(j,\nu)}$.*

This is an immediate consequence of the preceding lemmata.

Lemma 3.3. *Let $\omega_2 = \rho$ and $\rho + t_2^{(j)} \in \mathfrak{q}^j$. Then every prime ideal $\tilde{\mathfrak{q}} \ne \mathfrak{q}$ lying above q does not contain $\rho + t_2^{(j)}$.*

Proof. Let us assume that $\rho + t_2^{(j)} \in \tilde{\mathfrak{q}}$. Then we obtain $|o_F/\tilde{\mathfrak{q}}| = q$ and the prime ideal $\tilde{\mathfrak{q}}$ is of degree 1, too. Clearly, there is a congruence factorization

$$f(t) \ \equiv \ (t-m_1)\cdots(t-m_k)\, f_{k+1}(t)\cdots f_r(t) \bmod q\mathbb{Z}[t]$$

with pairwise distinct modulo q irreducible factors. A suitable ordering of those yields $m_1 \equiv t_2^{(j)} \bmod \mathfrak{q}$, $\mathfrak{q} = qo_F + (\rho - m_1)o_F$, and $\tilde{\mathfrak{q}} = qo_F + (\rho - m_2)o_F$. Without loss of generality we can assume that $0 \le m_i < q \quad (i = 1, 2)$. But then $\rho - t_2^{(j)} \in \tilde{\mathfrak{q}}$ has the consequence $m_1 - m_2 \in \tilde{\mathfrak{q}}$ with $0 <| m_1 - m_2 |< q$, a contradiction to $\tilde{\mathfrak{q}} \cap \mathbb{Z} = q\mathbb{Z}$. □

Lemma 3.4. *Let $\rho + t_2^{(j)} \in \mathfrak{q}^j$ and denote by $f_{\rho+t_2^{(j)}}(t) = t^n + \sum_{\mu=1}^{n} \lambda_\mu t^{n-\mu}$ the characteristic polynomial of $\rho + t_2^{(j)}$. For $1 \le \nu \le j$ a solution $b_\nu \in \,]-q^\nu/2,\, q^\nu/2[$ of the congruence $\lambda_n - q^j b_\nu \lambda_{n-1} \equiv 0 \bmod q^{j+\nu}$ satisfies $t_2^{(j+\nu)} = t_2^{(j)} + q^j b_\nu$.*

Proof. From the preceding lemma we know that $\rho + t_2^{(j+\nu)}$ is contained in exactly one prime ideal lying above q, namely $\mathfrak{q}$. Hence, $(\rho + t_2^{(j+\nu)})o_F = \mathfrak{q}^{j+\nu+\mu}\mathfrak{a}$ for a suitable non-negative integer μ, and q is not contained in any prime ideal dividing $\mathfrak{a}$. Taking norms on both sides we obtain $|N(\rho + t_2^{(j+\nu)})| = q^{j+\nu+\mu}N(\mathfrak{a})$ and q does not divide $N(\mathfrak{a})$. Therefore it suffices to choose b_ν such that $N(\rho + (t_2^{(j)} + q^j b_\nu))$ is divisible by $q^{j+\nu}$. Because

$$\begin{aligned} N(\rho + t_2^{(j+\nu)}) &= \prod_{k=1}^{n} (\rho^{(k)} + t_2^{(j)} + b_\nu q^j) \\ &= N(\rho + t_2^{(j)}) + b_\nu q^j \sum_{k=1}^{n} \frac{N(\rho + t_2^{(j)})}{\rho^{(k)} + t_2^{(j)}} + q^{2j}c \\ &= (-1)^n \lambda_n + b_\nu q^j (-1)^{n-1} \lambda_{n-1} + q^{2j}c, \end{aligned}$$

it suffices to choose b_ν as stated in the lemma. □

Remark. The calculation of the required coefficients of the characteristic polynomials is easy. Starting with $f(t) = f_\rho(t) = t^n + \sum_{i=1}^{n} a_i t^{n-i}$ we get $f_{\rho+\mu}(t) = f_\rho(t - \mu) = (t - \mu)^n + \sum_{i=1}^{n} a_i (t - \mu)^{n-i}$. The last two coefficients of that polynomial are

$$\lambda_n = (-\mu)^n + \sum_{i=1}^{n} a_i (-\mu)^{n-i}, \tag{3}$$

$$\lambda_{n-1} = \binom{n}{1}(-\mu)^{n-1} + \sum_{i=1}^{n-1} a_i \binom{n-i}{1}(-\mu)^{n-i-1}. \tag{4}$$

The other basis elements can then be updated easily.

If the underlying field is a global function field, only the following changes need to be made. (For the notation see also the subsequent section.) The norm of the chosen prime ideal $\mathfrak{q}$ becomes a monic irreducible polynomial $q(t)$. The constants t_k, $t_i^{(k)}$ will be replaced by polynomials whose degrees are bounded by k. Analogously, the intervals in the lemmata and the corollary are replaced by a degree bound ν.

4. The algorithm for global function fields

The geometry of numbers for (global) function fields differs from that of number fields inasmuch as these fields admit not a scalar product but only a norm. Hence, there is no

notion of LLL reduction. In order to define "good" bases of orders or ideals, we need to introduce a maximum norm as a kind of substitute for the T_2-norm of number fields. This concept was developed in the thesis of Schörnig (1996). It is based on earlier work by Schmidt (1991).

Let $\mathbb{F}_q(x)$ be the rational function field in the variable x over the field of q elements. Let K be a separable extension of $\mathbb{F}_q(x)$ of degree n. The places of $\mathbb{F}_q(x)$ will be denoted by lower case boldface letters, those of K by upper case boldface letters. The infinite place of $\mathbb{F}_q(x)$ that corresponds to the degree valuation is written as $\mathfrak{p}_\infty$. For $\mathfrak{P} \mid \mathfrak{p}$ the integers $e_{\mathfrak{P}|\mathfrak{p}}$, $f_{\mathfrak{P}|\mathfrak{p}}$ and $n_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$ denote the ramification index, the residue class degree and the local degree, respectively. $N(\mathfrak{P})$ is the number of elements in the residue class field of $\mathfrak{P}$. The exponential valuation belonging to $\mathfrak{P}$ is denoted by $\nu_{\mathfrak{P}}$. For every element $f \in K$ we then set

$$| f |_{\mathfrak{P}} := N(\mathfrak{P})^{-\nu_{\mathfrak{P}}(f)/n_{\mathfrak{P}|\mathfrak{p}}}.$$

This normalization has the effect that $| \ |_{\mathfrak{P}}$ is a prolongation of $| \ |_{\mathfrak{p}}$ and that the product formula is still valid.

Definition. The maximum norm of an element $f \in K$ is defined by

$$\| f \|_\infty := \max_{\mathfrak{P}|\mathfrak{p}_\infty} | f |_{\mathfrak{P}}.$$

The maximum norm has the familiar properties:

1. $\| f \|_\infty = 0 \Leftrightarrow f = 0$,
2. $\| \lambda f \|_\infty = | \lambda |_\infty \| f \|_\infty$,
3. $\| f + g \|_\infty \leq \max\{\| f \|_\infty, \| g \|_\infty\}$ and $\| f \|_\infty < \| g \|_\infty$ implies $\| f + g \|_\infty = \| g \|_\infty$ for all $f, g \in K$ and $\lambda \in \mathbb{F}_q(x)$.

As in the number field case we want to discuss the problem of factoring a polynomial $g(t) \in K[t]$ of degree $m := \deg(g) > 1$. We make the same assumptions as in Section 1: we assume that $g(t)$ is square-free, monic and has coefficients in $o_K[t]$. The generic algorithm can be applied similarly to in the number field case. Prime ideals of degree 1 are replaced by finite places of K of degree 1. The corresponding residue class mapping and Hensel's lifting procedure are straightforward. Hence, all we need to do is develop a strategy for recovering actual factors of $g(t)$ from the lifted ones.

We use the maximum norm to obtain suitable bounds for the size of the coefficients of potential factors of $g(t)$.

Lemma 4.1. *Let $g(t) = \sum_{i=0}^{m} g_i t^i \in o_K[t]$ be a monic polynomial of degree $m > 1$. For any place $\mathfrak{P}$ of K dividing $\mathfrak{p}_\infty$ we define a* measure *of the polynomial $g(t)$ by*

$$M_{\mathfrak{P}}(g) := \max\left\{ \sqrt[i]{| g_{m-i} |_{\mathfrak{P}}} \;\middle|\; 1 \leq i \leq m \right\}.$$

Then any polynomial $h(t) = \sum_{i=0}^{r} h_i t^i$ of $K[t]$ dividing $g(t)$ is monic, is in $o_K[t]$ and its coefficients h_i satisfy

$$| h_{r-i} |_{\mathfrak{P}} \leq M_{\mathfrak{P}}^i(g) \quad (1 \leq i \leq r).$$

Proof. The first statement holds since o_K is a Dedekind ring and therefore integrally closed.

The estimate for the coefficients of $h(t)$ is obtained by considering them as elementary symmetric functions of the zeros of $g(t)$. Let L be the splitting field of $g(t)$ over the completion $K_{\mathfrak{P}}$. The valuation $|\ |_{\mathfrak{P}}$ has a unique prolongation to L, which we also denote by $|\ |_{\mathfrak{P}}$. Let $\xi_1, \ldots, \xi_m$ be the zeros of $g(t)$ in L. We set

$$\tilde{M}_{\mathfrak{P}} := \max\{|\ \xi_i\ |_{\mathfrak{P}} \mid 1 \le i \le m\}$$

and

$$s := \sharp\{i \mid |\ \xi_i\ |_{\mathfrak{P}} = \tilde{M}_{\mathfrak{P}}\} \in \mathbb{Z}^{\ge 1}.$$

Then the coefficients h_{r-i} of $h(t)$ satisfy

$$|\ h_{r-i}\ |_{\mathfrak{P}} = \left| \sum_{1 \le j_1 < \cdots < j_i \le r} \xi_{j_1} \ldots \xi_{j_i} \right| \le \tilde{M}^i.$$

Because of $|\ g_{m-s}\ |_{\mathfrak{P}} = \tilde{M}^s$, we obtain $M_{\mathfrak{P}}(g) = \tilde{M}_{\mathfrak{P}}$ and thus the lemma. □

Corollary 4.1. *The coefficients h_i of a factor $h(t)$ of degree r of $g(t)$ in $o_K[t]$ satisfy*

$$\|\ h_i\ \|_\infty \le \max\{M^k_{\mathfrak{P}}(g) \mid 1 \le k \le r,\ \mathfrak{P} \mid \mathfrak{p}_\infty\} =: M(g) \quad (1 \le i \le r).$$

We note that the product formula yields $M(g) \ge 1$.

In the following we examine the relation between elements contained in the k-th power of a prime ideal $\mathfrak{Q}$ and their maximum norm.

Lemma 4.2. *Let $\mathfrak{Q}$ be a prime ideal of o_K lying above the prime ideal $\mathfrak{q}$ of $\mathbb{F}_q(x)$. Then any non-zero $\alpha \in o_K$ satisfies*

$$\|\ \alpha\ \|_\infty \ge |\ \alpha\ |_{\mathfrak{Q}}^{-n_{\mathfrak{Q}|\mathfrak{q}}/n}.$$

Proof. The product formula $\prod_{\mathfrak{P}} |\ \alpha\ |_{\mathfrak{P}}^{n_{\mathfrak{P}|\mathfrak{p}}} = 1$ and the property $|\ \alpha\ |_{\mathfrak{P}} \le 1$ for all $\mathfrak{P}$ not dividing $\mathfrak{p}_\infty$ yield

$$\|\ \alpha\ \|_\infty^n = (\max\{|\ \alpha\ |_{\mathfrak{P}} \mid \mathfrak{P} \mid \mathfrak{p}_\infty\})^n \ge \prod_{\mathfrak{P}|\mathfrak{p}_\infty} |\ \alpha\ |_{\mathfrak{P}}^{n_{\mathfrak{P}|\mathfrak{p}_\infty}} \ge |\ \alpha\ |_{\mathfrak{Q}}^{-n_{\mathfrak{Q}|\mathfrak{q}}} \ge 1. \quad \square$$

As in Section 2 we can now show that each residue class of o_K modulo $\mathfrak{Q}^k$ contains at most one element of bounded maximum norm provided that k is large enough.

Lemma 4.3. *Let $\mathfrak{Q}$ be a prime ideal of o_K lying above the prime ideal $\mathfrak{q}$ of $\mathbb{F}_q(x)$ and let $B > 1$. For $k \ge n \log(B)/\log(N(\mathfrak{Q}))$ every residue class of $o_K/\mathfrak{Q}^k$ contains at most one element α with $\|\ \alpha\ \|_\infty < B$.*

Proof. We assume that $\alpha, \beta \in o_K$ satisfy $\alpha + \mathfrak{Q}^k = \beta + \mathfrak{Q}^k$, $\alpha \ne \beta$, $\|\ \alpha\ \|_\infty \le \|\ \beta\ \|_\infty$. The result of the preceding lemma yields

$$\|\ \beta\ \|_\infty \ge \|\ \alpha - \beta\ \|_\infty \ge |\ \alpha - \beta\ |_{\mathfrak{Q}}^{-n_{\mathfrak{Q}|\mathfrak{q}}/n} = N(\mathfrak{Q})^{v_{\mathfrak{Q}}(\alpha-\beta)/n} \ge N(\mathfrak{Q})^{k/n}. \quad \square$$

What we still need for carrying out Step 4 of the generic algorithm in the function field case is a method for computing an element of smallest maximum norm in a residue class of o_K modulo $\mathfrak{O}^k$. The methods applied in the case of number fields cannot be used since they are based on the T_2-norm coming from a positive definite quadratic form. As a substitute we apply the basis reduction algorithm developed in Schörnig (1996). We recall that any non-zero ideal $\mathfrak{A}$ of o_K is a free $\mathbb{F}_q[x]$-module of rank n, a basis for which can be computed analogously to the number field case.

We call a basis $v_1, \ldots, v_n$ of $\mathfrak{A}$ reduced if the representation $v = \sum_{i=1}^{n} \lambda_i v_i$ of any $v \in \mathfrak{A}$ (i.e., $\lambda_i \in \mathbb{F}_q[x]$) satisfies

$$\| v \|_\infty = \max\{ | \lambda_i |_\infty \| v_i \|_\infty \mid 1 \le i \le n \}.$$

We note that the 0-reduced bases defined in Schörnig (1996) are also reduced with respect to our definition. For the case of $K/\mathbb{F}_q(x)$ tamely ramified, Schörnig developed an efficient algorithm for computing reduced bases.

The notion of reduced bases of an ideal $\mathfrak{A}$ of o_K yields an easy way to compute an element of smallest maximum norm in each residue class of $o_K/\mathfrak{A}$. Let $\alpha \in o_K$, $v \in \mathfrak{A}$ and $v_1, \ldots, v_n$ be a reduced basis of the non-zero ideal $\mathfrak{A}$ of o_K. Then we have representations $v = \sum_{i=1}^{n} \lambda_i v_i$ and $\alpha = \sum_{i=1}^{n} \frac{\sigma_i}{\tau_i} v_i$ with $\lambda_i, \sigma_i, \tau_i \in \mathbb{F}_q[x]$ that can easily be calculated. We want to determine an element of smallest maximum norm in $\alpha + \mathfrak{A}$. Since our basis $v_1, \ldots, v_n$ is reduced, we obtain

$$\| \alpha + v \|_\infty = \max \left\{ \left| \lambda_i + \frac{\sigma_i}{\tau_i} \right|_\infty \| v_i \|_\infty \;\middle|\; 1 \le i \le n \right\}.$$

Hence, we need to choose the λ_i such that the first factor becomes as small as possible. Clearly, this is achieved if we carry out a division with remainder of σ_i, τ_i in $\mathbb{F}_q[x]$. We get $\sigma_i = \gamma_i \tau_i + \delta_i$ with $\deg(\delta_i) < \deg(\tau_i)$. Setting $\lambda_i = -\gamma_i$ we obtain for the first factor an optimal lower bound

$$\left| \lambda_i + \frac{\sigma_i}{\tau_i} \right|_\infty = q^{\deg(\delta_i) - \deg(\tau_i)}.$$

This puts us into a situation in which we can apply the generic factoring algorithm of Section 1 in the function field case also.

Acknowledgements

The author thanks the referees for their inspiring criticism of earlier versions of the manuscript.

References

Bach, E., Shallit, J., 1996. Algorithmic Number Theory, vol. 1. MIT Press, Cambridge.

Beauzamy, B., 1992. Products of polynomials and a priori estimates for coefficients in polynomial decompositions: a sharp result. J. Symbolic Comput. 13, 463–472.

Daberkow, M., Fieker, C., Klüners, J., Pohst, M., Roegner, K., Schörnig, M., Wildanger, K., 1997. KANT V4. J. Symbolic Comput. 24, 267–283.

Encarnación, M.J., 1997. Factoring polynomials over algebraic number fields via norms. In: Küchlin, W. (Ed.), Proc. ISSAC 97. ACM Press, pp. 265–270.

Fieker, C., Friedrichs, C., 2000. On reconstruction of algebraic numbers. In: Bosma, W. (Ed.), Proc. ANTS IV. LNCS, 1838, Springer, pp. 285–296.

Lenstra, A.K., 1982. Lattices and factorization of polynomials over algebraic number fields. In: Proc. Eurocam'82. LNCS, 144, Springer, pp. 32–39.

Lenstra, A.K., Lenstra Jr., H.W., Lovasz, L., 1982. Factoring polynomials with rational coefficients. Math. Ann. 261, 515–534.

Mignotte, M., 1974. An inequality about factors of polynomials. Math. Comp. 28, 1153–1157.

Pohst, M., 1993. Computational Algebraic Number Theory. Birkhäuser Verlag, Basel.

Pohst, M., Zassenhaus, H., 1989. Algorithmic Algebraic Number Theory. Cambridge University Press, Cambridge.

Roblot, X.-F., 1997. Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction de corps de classes de rayon. Thèse, L'Université Bordeaux I.

Schmidt, W.M., 1991. Construction and estimation of bases in function fields. J. Number Theory 39, 181–224.

Schörnig, M., 1996. Untersuchungen konstruktiver Probleme in globalen Funktionenkörpern. Thesis, TU Berlin.

Stoer, J., Bulirsch, R., 1993. Introduction to Numerical Analysis, 2nd ed. Springer.

Trager, B.M., 1976. Algebraic factoring and rational function integration. In: Proc. 1976 Symp. on Symbolic and Algebraic Computation. ACM Press, pp. 219–226.

Weinberger, P.J., Rothschild, L.P., 1976. Factoring polynomials over algebraic number fields. ACM Trans. Math. Software 2, 335–350.